UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA,

- against - 14 Cr. 160 (SAS)

FRANK DITOMASSO,

Defendant.

----------X

SUPPLEMENTAL MEMORANDUM OF LAW REGARDING WHETHER OMEGLE'S MONITORING CONSTITUTED A "PRIVATE SEARCH"

INTRODUCTION

As directed by the Court in its opinion and order filed October 28, 2014 (hereainafter "D.E. 23") Frank DiTomasso submits the within supplemental memorandum of law to address "whether Omegle's monitoring of DiTomasso's chats was a 'private search,' outside the bounds of constitutional protection, or whether it was a search carried out at the behest of law enforcement, which would trigger Fourth Amendment scrutiny." D.E. 23 at 28. For the reasons set forth herein, the facts and circumstance preclude the conclusion that Omegle's actions constituted a "private search" as that concept has been defined in Fourth Amendment jurisprudence.

DISCUSSION

First, it is important note at the outset of this discussion, that the warrantless monitoring of its subscribers' "chats" that Omegle utilizes would, if conducted by law enforcement agents, be a blatant violation of the Fourth Amendment. If as its policy statements assert, Omegle's screen captures involve real time, warrantless monitoring of subscribers' electronic communications (video chats), it is an apparent violation of the Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000). Thus, it is questionable if even screen captures performed for exclusively non-law-enforcement purposes would be a legally permissible option for Omegle.

In any event, once they are maintained and stored in a digital form, "screen captures" are functionally indistinguishable from an e-mail, and, therefore, are subject to the same Fourth Amendment expectation of privacy as the content of an e-mail. Indeed, to compel a provider of ECS to disclose contents of communications in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant. 18 U.S.C. § 2703(a).

Second, the absence of an explicit request addressed specifically to Omegle to monitor its subscribers' chats does not compel a finding that such monitoring was a " 'private search' outside the bounds of constitutional protection." To the contrary, the government may become a party to a search through nothing more than tacit approval. *Lustig v. United States*, 338 U.S. 74, 78-79 (1949)(plurality opinion); *United States v. Knoll*, 116 F.3d 1313, 1320 (2d Cir. 1994); 1 Wayne R. LaFave, Search & Seizure § 1.8(b).

Third, a search may lose its wholly private character --and the private party may become in effect a government agent -- once the private party expands the purpose of the search to include obtaining evidence for law enforcement. As the Second Circuit observed in *Knoll*, 116 F.3d at 1320, for example:

> A private party acting as a government agent also may not expand upon a previously private search without running afoul of the Fourth Amendment. Although here the burglary may have been accomplished, that is, the boxes of documents had been stolen from Knoll's office before the government knew of the burglary, the search itself may not have been complete until Devany, upon Ernle's and ultimately AUSA Bruce's request, went through all the stolen files and listened to the tapes to find the material to be turned over to the FBI to be used against Knoll and Gleave. At some point in the ongoing search, Ernle and Devany may have been acting as agents of the government given that AUSA Bruce directed their actions and tacitly approved of whatever measures they took to produce information he wanted from the contents of the files.

Assuming *arguendo* that Omegle initially has a non-law-enforcement reason for taking screen captures, once it expands, in particular instances, the purposes for which it conducts human review of particular sets of screen captures – to include violation of criminal laws as well violations of its internal policy – Omegle crosses the line from conducting a wholly private search to conducting a search as an agent of law enforcement.

In other words, in this case, once – due to the mandatory reporting requirement of 18 U.S.C. § 2258A(e) – the review of screen captures began to serve the purposes of law enforcement as well Omegle's unrelated purposes, Omegle became an agent or instrumentality of law enforcement, and concomitantly law enforcement participated vicariously in Omegle's search. *Cf*: *State v. Scrotsky*, 39 N.J. 410, 189 A.2d 23 (N.J. Sup. Ct. 1963) (where landlady and police officer entered her tenant's apartment without a warrant – she seeking property her tenant had stolen from her and the police officer seeking evidence of that crime, "[t]he search and seizure by one served the purpose of both, and must be deemed to have been participated in by both.").

Indeed, an ISP that inadvertently, or in the course of conducting some sort of anti-spam initiative or statistical analysis of the traffic on its servers, stumbles upon child pornography is not free to deal with the child pornography problem as a wholly private matter. To the contrary, the ISP must report the offending material and the person or persons who sent or received the pornography to law enforcement, albeit via the NMEC, under pain of criminal penalties. In addition, it must effectively preserve the evidence on law enforcement's behalf, securing it until law enforcement can begin the process necessary to acquire it. Given that an ISP is not free to deal with the problem child pornography privately on its terms, the private search doctrine makes no sense in this unique context. Perhaps this point is best illustrated by the following comparison.

Assume a landlord found that a person renting a house from him was storing suspected contraband -- e.g., illegal drugs, chemicals, weapons, or even child pornography. If the landlord goes to the police, the tenant may be arrested and publicly charged, and the landlord may suffer

public embarrassment or suffer economic loss as the result of having one of his properties associated with the contraband. The landlord can avoid such adverse consequences, by employing wholly private measures, without getting the police involved. For example, the landlord can simply ask the tenant to leave and take his contraband with him. In sharp contrast, an ISP cannot treat the problem as a wholly private matter.

To the contrary, an ISP that finds "any facts or circumstances from which there is an apparent violation" of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography must file a report. 18 U.S.C. § 2258A (a)(1) & (2). Unlike the landlord who can tell his tenant to remove himself and his contraband from the premises, the ISP apparently cannot discuss the matter with the subscriber who is the subject of the mandatory report. 18 U.S.C. § 2258A (g)(2)(B)(i) ("LIMITATIONS ON FURTHER DISCLOSURE.—The electronic communication service provider or remote computing service provider shall be prohibited from disclosing the contents of a report provided under subparagraph (A)(vi) to any person, except as necessary to respond to the legal process.").

This prohibition alone would suffice to deter an ISP from even attempting to discuss the matter with the subscriber named in a report mandated by 18 U.S.C. § 2258A in an effort to rid itself of the subscriber through wholly private action. However, there are further obstacles to private action.

Unlike the landlord of a house, the ISP cannot simply, privately and quietly remove the offending matter from its server because the ISP's notification to NCMEC "shall be treated as a request to preserve as if such request was made pursuant to section 2703(f). " 18 U.S.C.

§ 2258A (h)(1). The ISP must also maintain the offending images as well as any images, data, or other digital files that are commingled or interspersed among the images of apparent child pornography."

Indeed, 18 U.S.C. § 2258A (h), in effect mandates an ISP to "seize" (in the Fourth Amendment sense of that word) apparent child pornography as well as any commingled images data or digital files. Surely these seizures cannot be described as wholly private action on the part of the ISPs. To the contrary this is an obvious seizure of the offending material for law enforcement purposes, and this is a seizure moreover, that is made at the instigation, indeed the compulsion, of a federal criminal statute.

CONCLUSION

In summary, the private search exception, assumes that a private actor has the option of not reporting to, and seizing for law enforcement agents, evidence of a crime that the private party happens upon in the course of his personal or business affairs. However, when it comes child pornography, ISPs and other information service providers do not have any option but to search and report evidence that appears to be child pornography to law enforcement. Thus, it is impossible to have a truly private search in this context.

Dated: New York, New York
November 3, 2014

Respectfully Submitted,

/s/ Lee A. Ginsberg

Lee A. Ginsberg
FREEMAN, NOOTER & GINSBERG
75 Maiden Lane, Suite 503
New York, New York 10038
(212) 608-0808

Attorney for Defendant